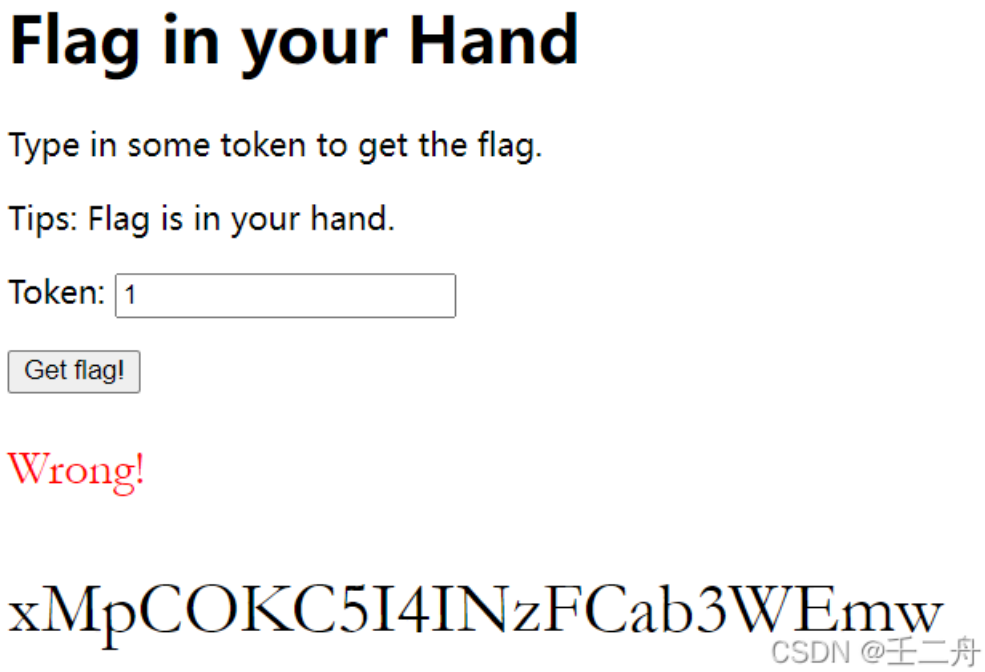
攻防世界 flag_in_your_hand

原创

仲鳌 于 2022-03-11 16:59:15 发布 1295 收藏 1
分类专栏： CTF 文章标签： javascript safari webview

下载附件打开文件中的html文件

无论输入什么都是错误



我们打开网页源代码看看

```
<html>
 <head>
  <title>Flag in your Hand</title>
  <style type="text/css">
   body {
    padding-left: 30%;
   }

   #flag {
    font-family: Garamond, serif;
    font-size: 36px;
   }

   #flagtitle {
    font-family: Garamond, serif;
    font-size: 24px;
   }

   .rightflag {
    color: green;
   }

   .wrongflag {
    color: red;
   }
  </style>
  <script src="script-min.js"></script>
  <script type="text/javascript">
   var ic = false;
   var fg = "";

   function getFlag() {
    var token = document.getElementById("secToken").value;
    ic = checkToken(token);
    fg = bm(token);
    showFlag()
```

```
   }

   function showFlag() {
    var t = document.getElementById("flagTitle");
    var f = document.getElementById("flag");
    t.innerText = !!ic ? "You got the flag below!!" : "Wrong!";
    t.className = !!ic ? "rightflag" : "wrongflag";
    f.innerText = fg;
   }
  </script>
 </head>
 <body>
  <h1>Flag in your Hand</h1>
  <p>Type in some token to get the flag.</p>
  <p>Tips: Flag is in your hand.</p>
  <div>
   <p>
    <span>Token:</span>
    <span><input type="text" id="secToken"/></span>
   </p>
   <p>
    <input type="button" value="Get flag!" onclick="getFlag()" />
   </p>
  </div>
  <div>
   <p id="flagTitle"></p>
   <p id="flag"></p>
  </div>
 </body>
</html>
```

获得flag

```
function getFlag() {
    var token = document.getElementById("secToken").value;
    ic = checkToken(token);
    fg = bm(token);
    showFlag()
   }
```

输出flag

```
function showFlag() {
    var t = document.getElementById("flagTitle");
    var f = document.getElementById("flag");
    t.innerText = !!ic ? "You got the flag below!!" : "Wrong!";//判断ic是true还是flase
    t.className = !!ic ? "rightflag" : "wrongflag";
    f.innerText = fg;
   }
```

然后我们查看script-min.js其中改变ic的值的

```
function ck(s) {
    try {
        ic
    } catch (e) {
        return;
    }
    var a = [118, 104, 102, 120, 117, 108, 119, 124, 48,123,101,120];
    if (s.length == a.length) {
        for (i = 0; i < s.length; i++) {
            if (a[i] - s.charCodeAt(i) != 3)
                return ic = false;
        }
        return ic = true;
    }
    return ic = false;
}
```

我们读代码发现当a-我们输入的字符串等于3的时候ic就是true所以我们把它翻过来我这里用python写的

```
a=[118, 104, 102, 120, 117, 108, 119, 124, 48, 123, 101, 120]
b=''
for i in a:
 b+=chr(i-3)
print(b)
```

运行一下

得出结果

```
security-xbu
```

我们返回html输入这个值

Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token: security-xbu

Get flag!

You got the flag below!!

RenIbyd8Fgg5hawvQm7TDQ

就得出了，flag

```
RenIbyd8Fgg5hawvQm7TDQ
```